Iwasawa theory and Selmer schemes II
- verifying the dimension hypothesis -

Dohyeong Kim

Seoul National University

May 18, 2022

Iwasawa theory and p-adic L-functions

Motivation: the non-abelian Chabauty program

The dimension hypothesis in the title originates from the non-abelian Chabauty program.

Last week, we started with Selmer groups for elliptic curves where things are non-hyperbolic and groups are abelian. Today, we adopt a complementary point of view by starting with abelian and hyperbolic case with an additional assumption on the rank.

(abelian) Chabauty - when the rank is low

Let $X/\mathbb{Q}$ be a curve of genus $g \geq 2$, with a fixed base-point $b \in X(\mathbb{Q})$. Assume that the Jacobian $J_X/\mathbb{Q}$ has rank at most $g-1$. Then, for some 1-form ω over $\mathbb{Q}_p$,

$$\int_b^- \omega \colon X(\mathbb{Q}_p) \to \mathbb{Q}_p \qquad (1)$$

is non-trivial and vanish on $X(\mathbb{Q})$.
Zeros of a non-trivial such funtion are discrete and $X(\mathbb{Q}_p)$ is compact. It follows that $X(\mathbb{Q})$ is finite.

The dimension hypothesis

The rank hypothesis is not satisfied in general, so one needs to work under a weaker hypothesis and allow other functions. In fact, an iterated integral

$$\int_b^- \omega_1 \cdot \omega_2 \cdot \cdots \cdot \omega_n \colon X(\mathbb{Q}_p) \to \mathbb{Q}_p \tag{2}$$

would exist if the dimension hypothesis is satisfied. This extends to a number field F, the non-triviality of the function is delicate unless $F \neq \mathbb{Q}$. See Hast's 2021 paper on "functional transcendence..".

Unlike the rank hypothesis, the dimension hypothesis is expected to hold true all the time. Indeed, there are several conditional proofs and some unconditional proofs of special cases.

The statement

Let S be a sufficiently large finite set of places of F. Let v be a place of F dividing p. We have

$$\dim_{\mathbb{Q}_p} H^1_f\left(G_S(F), U_n^{\text{ét}}\right) < \dim_{\mathbb{Q}_p} \mathrm{Res}^{F_v}_{\mathbb{Q}_p}\left(U_n^{\mathrm{dR}}/\mathrm{Fil}^0 U_n^{\mathrm{dR}}\right) \tag{3}$$

for all $n \gg 1$.

The terms need to be defined, but our interest lies in the hypotheses of conditional proofs. We are unable to produce a full proof, but we claim that our assumptions are milder.

Conditional Proof - M. Kim (2009)

Let X/F be a smooth projective curve. Define

$$\mathrm{Sel}^0_S(F,W) = \ker\left(H^1(G_S(F),W) \to \bigoplus_{v\in S} H^1(F_v,W)\right) \tag{4}$$

for a Galois representation W unramified outside S.

Hypothesis

Put $V_n = H^1_{\acute{e}t}(X_{\overline{F}},\mathbb{Q}_p)^{\otimes n}(1)$. Then, $\mathrm{Sel}^0_S(F,V_n) = 0$ for all $n \gg 1$

Plan

Our plan is to give a conditional proof of the hypothesis.

What is the point?

For a generic curve, our contribution is negligible. For a specific curve, our condition can be checked, at least in theory. We give a numerical example later.

Preliminaries

For a profinite group $\mathcal{G}$, denote its Iwasawa algebra by $\Lambda(\mathcal{G})$. For now, let K be a number field.

Suppose that there is a p-adic Lie extension K_∞/K containing the cyclotomic $\mathbb{Z}_p$-extension K^{cyc}/K. Put $G = \mathrm{Gal}(K_\infty/K)$, $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$, and $\Gamma = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$. By Galois theory, we identify $G/H = \Gamma$. Here is an important class of modules in the non-commutative Iwasawa theory.

Definition

We say a module over $\Lambda(G)$ belongs to the category $\mathfrak{M}_H(G)$ if it is finitely generated over $\Lambda(H)$.

Important special case is when $H = \{1\}$, where an Iwasawa module beloongs to $\mathfrak{M}_H(G)$ if and only if its μ-invariant is zero.

Fine Selmer group

Let M_∞/K_∞ be the largest abelian p-extension in which all places lying above p split completely in M_∞. Define

$$Y(K_\infty/K) = \mathrm{Gal}(M_\infty/K_\infty) \tag{5}$$

which is a $\Lambda(G)$-module.

Hypothesis(Coates–Sujatha)

Assume that p is odd. Then, $Y(K_\infty/K)$ belongs to the category $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$.

Special case

We are interested in the special case when F_∞/F is obtained from the p-power division points of an abelian variety A.

Recall that we have a short exact sequence of groups

$$1 \to H \to G \to \Gamma \to 1 \tag{6}$$

which is always a semi-direct product.

Not a product in general - a false Tate curve extension gives an open subgroup of $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$.

A nice splitting

We say a splitting $s\colon \Gamma \to G$ of

$$1 \to H \to G \to \Gamma \to 1 \tag{7}$$

is *nice if* $s(\Gamma)$ *is contained in the center of* $GL_{2g}(\mathbb{Z})$*, where one regards* $G \subset GL_{2g}(\mathbb{Z}_p)$*. The embedding is well-defined up to conjugation and so is a section being nice.*

I am interested in the nice sections on some open subgroup of Γ*.*

Why should it exist?

If A is a CM elliptic curve, there are non-nice sections. However, nice sections always exist, too.

If A is a non-CM elliptic curve, there is such a section because of Serre's Open Image Theorem.

It looks like an overkill to me, but I do not know any other proofs.

Other extreme case

The subgroup $G \subset \mathrm{GL}_{2g}(\mathbb{Z}_p)$ 'should' have a finite index in the Mumford-Tate group. There are several partial results in varying restrictions on the dimension and the type of the group. The largest possible is GSp_{2g}, in which case there is a proof by C. Hall (2011) under a hypothesis on the Néron model.

Vasiu 2008

Vasiu proved a theorem that amounts to the existence of a nice splitting in all cases. One can regard it as a fairly weak, still highly non-trivial, generalization of Serre's Open Image Theorem.

Why nice splitting matters

Let T be a $\Lambda(G)$-module which belongs to the category $\mathfrak{M}_H(G)$. View $G = H \times \Gamma$ via the choice of a nice section. Then $\bar{T} = T \otimes \overline{\mathbb{Q}}_p$ decomposes into a finite number of Γ-isopytic components

$$\bar{T} = \bigoplus_{\psi} \bar{T}^{\psi} \tag{8}$$

where $\psi \colon \Gamma \to \overline{\mathbb{Q}}_p^{\times}$ is a character.

Why nice splitting matters

Let $G = \mathrm{Gal}(F_\infty/F)$. Recall $V_n = H^1_{\text{ét}}(X_{\overline{F}}, \mathbb{Q}_p)^{\otimes n}(1)$. Then, Γ acts on V_n isotypically of type, say, ψ_n. Moreover, $\psi_1, \psi_2, \cdots$ are all distinct. So only a finite number of them can appear in the decomposition

$$\bar{T} = \bigoplus_{\psi} \bar{T}^{\psi} \tag{9}$$

meaning that

$$\mathrm{Hom}_{\Lambda(G)}(T, V_n) = 0 \tag{10}$$

for all $n \gg 1$.

A standard use of the Hochschild-Serre spectral sequence and taking care of places not dividing p, one obtains the “Hypothesis”, when $Y(F_\infty/F)$ belongs to the category $\mathfrak{M}_H(G)$.

Reduction to the commutative case

The $\mathfrak{M}_H(G)$-conjecture is convenient to work with for the following reason.

Theorem (Coates-Sujatha)

If $F\infty/F$ is pro-p, then $Y(F_\infty/F)$ belongs to the category $\mathfrak{M}_H(G)$ is and only if so does $Y(F_{cyc}/F)$.

If $F/\mathbb{Q}$ is abelian, than $\mu = 0$ and the main conjecture implies that F_{cyc}/F belongs to the category $\mathfrak{M}_H(G)$.

Applications

In the next few slides, I will show you some numerical examples and try to convince that our criterion is not entirely useless.

Example #0

Example

Let E_0 be the elliptic curve defined by the equation

$$E_0 \colon y^2 + xy + y = x^3 - 75x + 242$$

whose label is '1862.a1' in both the Cremona Database and LMFDB. It has a point of order three. Take $p = 3$ and $F = \mathbb{Q}(\mu_3)$. Then F_∞/F is pro-3. Moreover, F satisfies Iwasawa's hypothesis. Its rank over $\mathbb{Q}$ is two.

Example #1

Example

Let E_1 be the elliptic curve defined by the equation

$$E_1 \colon y^2 + xy = x^3 - 1282x + 36036$$

whose label is '216634.c1' in LMFDB(Cremona label 216634a1). It has a point of order three. Again take $p = 3$ and $F = \mathbb{Q}(\mu_3)$. Then F_∞/F is pro-3. Moreover, F satisfies Iwasawa's hypothesis. Its rank over $\mathbb{Q}$ is three.

Example #2

Example

Let E_2 be the elliptic curve defined by the equation

$$E_2\colon y^2 + xy + y = x^3 + x^2 - 2365x + 43251$$

whose label is '5302.h2' in LMFDB(Cremona label 5302i1). Take $p = 5$ and $F = \mathbb{Q}(\mu_5)$. Then F_∞/F is pro-5. Moreover, F satisfies Iwasawa's hypothesis. Its rank over $\mathbb{Q}$ is three.

How many such examples?

Elliptic curves over $\mathbb{Q}$ with large rank with restriction on its torsion subgroup have been studied but we it seems to be unknown whether there are infinitely many curves with point of order $p = 7$ and rank at least two. If $p = 3, 5$, there are infinitely many curves with rank at least two.

I found the database maintained by Andrej Dujella useful.

Example #3

I have only one genus two example, taken from a paper by Bruin–Flynn–Testa: the Jacobian of the curve

$$y^2 = (13x^3 - 105)^2 - 12(x^2 - 3x - 3)^3$$

rational isotropic subgroup isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$. So $F_\infty/F(\mu_3)$ is pro-3 and we are done.

Thank You!